Securing Your Web World

Trend Micro™

Vulnerability Management Services

Automated vulnerability and risk management powered by Qualys

Security compliance is costly, complex, and ever changing. Protecting your company data and reputation remains a challenge. Understanding your overall security posture—and doing so in relation to compliance requirements—has historically been time consuming, not to mention costly to implement, difficult to manage, and limited in terms of cross-functional information use. Enterprises need streamlined solutions that automate the vulnerability management process, facilitate optimum IT operations, and support time-consuming audits.

Trend Micro Vulnerability Management Services automates the process of vulnerability management and policy compliance across the enterprise, providing network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Policy compliance features allow security managers to audit, enforce and document compliance with internal security policies and external regulations. And it's easy to implement. As an on demand Software-as-a-Service (SaaS) solution, there is no infrastructure to deploy or manage.

AUTOMATING VULNERABILITY MANAGEMENT

Trend Micro Vulnerability Management Services automates the lifecycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, asset prioritization, and vulnerability assessment reporting. Vulnerability Management Services allows administrators to audit, enforce and document network security in accordance with internal policies and external regulations—providing comprehensive reports on vulnerabilities including severity levels, time to fix estimates, and impact on business.

ENFORCING IT POLICY COMPLIANCE

Vulnerability Management Services automates the collection of OS configuration and application access controls from information assets within the enterprise. The services also provide compliance reporting by leveraging a comprehensive knowledgebase of technical controls that are mapped to prevalent security regulations, industry standards, and compliance frameworks.

SCANNING WEB APPLICATIONS FOR FLAWS

Vulnerability Management Services provides automated crawling and testing for web applications and custom code to identify most vulnerabilities, such as those in the OWASP Top 10 and WASC Threat Classification, including SQL Injection and Cross-Site Scripting. It's easy to manage web applications, launch scans, and generate reports using a simple web portal.

MAINTAINING PCI DSS COMPLIANCE

Vulnerability Management Services provides businesses, online merchants and Member Service Providers the easiest, most cost-effective and highly automated way to achieve Payment Card Industry Data Security Standard (PCI DSS) compliance. The services streamline business operations related to PCI compliance and validation for merchants and acquirers, all from a combined collaborative application with automated report sharing and distribution.

SOFTWARE-AS-A-SERVICE

Protection Points

- Internet facing servers
- Internal clients and servers
- Networks

Threat Protection

- Vulnerability and risk management
- Regulatory compliance

KEY BENEFITS

Mitigates risk
Automates vulnerability identification and prioritizes remediation based on risk to business operations.

Streamlines audits
Offers customizable, agent-less auditing scans from a single interface with least impact to IT resources.

Saves money
Reduces capital expenditures, human resources, maintenance, and infrastructure with on-demand SaaS technology.

Provides immediate visibility
Allows IT to rapidly identify, visualize, and organize network assets and risk profiles by Business Unit and Asset Group.

Centralized policy definition
Consolidates IT compliance and security processes into a single solution.

Secures web applications
Identifies vulnerabilities of syntax and semantics in any number of web applications.

Simplifies compliance
Discovers IT assets and compares their configurations against standards to help organizations audit and define corrective actions.

FEATURES

Endpoint Security Platform Agent

- **Centralized vulnerability management.** Automates centralized reporting from distributed scans and consolidates administration of both internal and external (perimeter) scanning
- **Automation.** Offers scheduled scans and network discoveries as well as automated daily updates to a vulnerability KnowledgeBase and automated remediation ticket generation and verification
- **Accuracy.** Provides trusted, third-party certification of network security with tamper resistant audit trails supported by thousands of unique checks using non-intrusive scanning techniques
- **Comprehensive view.** Delivers a 360-degree view of network vulnerabilities using internal and external scanning as well as un-trusted and authenticated scanning
- **Reporting.** Automates reporting across all scan data, including detailed patch reports, customizable trending, differential and scorecard summary reports by asset group, user, and vulnerability
- **Interoperability.** Features extensible XML API Library, out-of-the-box integration with leading SIM solutions, helpdesk systems, and patch management systems for auto-remediation
- **Industry standard.** Supports vulnerability scoring with Common Vulnerability Scoring System (CVSS) as well as the addition of custom detections using Open Vulnerability Assessment Language (OVAL)

Policy Compliance

- **Technical Controls library.** Continuously maintains controls based on CIS and NIST standards and maps to many frameworks and regulations such as COBIT, ISO, ITIL, FFIEC, and NERC
- **Policy editor.** Constructs policies from controls and maps them to internal standards and external regulations
- **Compliance report templates.** Show compliance by policy, by control, and by host
- **Exception management workflow.** Facilitates the creating, evaluating, and approving risk acceptance of policy violations
- **Collaboration capabilities.** Allows the review of policies and approval of exceptions with internal and external auditors

Web Application Scanning

- **Crawling and link discovery.** Includes embedded web crawler which automatically crawls web applications and balances breadth and depth of assessment across discovered links
- **Blacklist/Whitelist.** Prevents the crawler from visiting certain links in a web application and instructs the crawler to only visit links explicitly defined in this list
- **Performance tuning.** Employs user-determined bandwidth level for parallel scanning to control impact on application performance
- **Sensitive content.** Enables automated expression search for content in HTML, such as Social Security Number
- **Workflows.** Provides logical workflows for defining scans and reviewing reports to provide deep visibility on vulnerabilities for each web application

PCI Compliance

- **Fully integrated self-assessment questionnaire.** Provides an online version of the PCI Security Council Self-Assessment Questionnaire (SAQ v1.2) that can be collaboratively viewed and shared by multiple users, including partners and merchants
- **On-demand network security scans.** Keeps PCI DSS-defined vulnerabilities continuously up to date with scans that are scheduled to run automatically or performed on demand
- **Compliance reporting and submission.** Automatically generates reports that can be used to identify and prioritize remediation or submitted as proof of PCI compliance
- **Web application scanning.** Secures web applications to meet PCI requirements by scanning vulnerability types within any application
- **Remediation.** Streamlines vulnerability remediation through comprehensive, step-by-step instructions with follow-up scans for seamless verification of remediation efforts

COMPLEMENTARY SERVICES

- Threat Management Services (post-incident malware assessment)

COMPLEMENTARY SOLUTIONS

- Deep Security (host based virtual patching/shielding)
- Endpoint Security Platform (patch management)

www.trendmicro.com